http://dx.doi.org/10.35596/1729-7648-2020-18-6-81-87

Оригинальная статья
Original paper

УДК 004.056.5; 621.396.21

СИНТЕЗ ИЗМЕРИТЕЛЬНОГО КОМПОЗИТНОГО СИГНАЛА ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕЧЕВЫХ СИГНАЛОВ ПРИ ДИСКРЕТНО-КВАНТОВАННОМ ПРЕОБРАЗОВАНИИ

ЖЕЛЕЗНЯК В.К.[1], ЛАВРОВ С.В.[1], ФИЛИППОВИЧ А.Г.[2], БАРАНОВСКИЙ М.М.[2]

[1]*Полоцкий государственный университет (г. Новополоцк, Республика Беларусь)*

[2]*Оперативно-аналитический центр при Президенте Республики Беларусь (г. Минск, Республика Беларусь)*

Поступила в редакцию 20 августа 2020

Аннотация. Цель работы – системно проанализировать и обобщить высокоточный измерительный сигнал для оценки защищенности в каналах утечки в шумах высокого уровня дискретно-квантованным представлением речевых сигналов принципами амплитудно-импульсной модуляции. Установлено, что дискретизация по времени и квантование по уровню высокоскоростных высококачественных речевых сигналов для преобразования в цифровую форму являются основными источниками утечки информации. Показано, что для определения степени защищенности информации при высококачественной высокоскоростной передаче в широкополосных каналах передачи информации необходимо использовать сложный измерительный (тестовый) композитный сигнал. Требования к измерительному сигналу определяются особенностями дискретно-квантованного представления речевых сигналов. В качестве измерительного сигнала предложено использовать периодическую импульсную последовательность треугольной формы. Измерительный сигнал треугольной формы имеет преимущество перед гармоническим сигналом в процессе выделения шума квантования, так как позволяет достичь более высокой точности при его обработке. Для оценки защищенности канала, обусловленного амплитудно-импульсной модуляцией, используется гармонический сигнал, сформированный из периодической импульсной последовательности треугольной формы методом преобразования Фурье. Использование предложенного измерительного композитного сигнала позволяет установить его численную зависимость с численным значением сигнала, принятого в качестве нормированного, и сравнить для принятия решения о защищенности речевого сигнала. Представленные в статье материалы являются оригинальными и могут быть использованы при оценке защищенности каналов утечки речевых сигналов, преобразованных в цифровую форму. Кроме того, полученные результаты позволяют проводить дальнейшие исследования защищенности речевых сигналов при их обратном преобразовании из цифровой формы в исходный сигнал.

Ключевые слова: защита информации, канал утечки речевого сигнала, дискретно-квантованный, композитный сигнал.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Железняк В.К., Лавров С.В., Филиппович А.Г., Барановский М.М. Синтез измерительного композитного сигнала для оценки защищенности речевых сигналов при дискретно-квантованном преобразовании. Доклады БГУИР. 2020; 18(6): 81-87.

SYNTHESIS OF A MEASURING COMPOSITE SIGNAL FOR ASSESSING THE SECURITY OF SPEECH SIGNALS DURING DISCRETE-QUANTIZED TRANSFORMATION

VLADIMIR K. ZHELEZNJAK[1], SERGEI V. LAVROV[1], ANDREI G. FILIPOVICH[2], MIKHAIL M. BARANOUSKI[2]

[1]*Polotsk State University (Novopolotsk, Republic of Belarus)*

[2]*Operational and Analytical Center under the Aegis of the President of the Republic of Belarus (Minsk, Republic of Belarus)*

Submitted 20 August 2020

Abstract. The purpose of the work is to systematically analyze and generalize a high-precision measuring signal for assessing the security in leakage channels in high-level noise by discrete-quantized representation of speech signals using the principles of amplitude-pulse modulation. It has been established that time sampling and level quantization of high-speed high-quality speech signals for digitalization are the main sources of information leakage. It is shown that to determine the degree of information security for high-quality high-speed transmission in broadband information transmission channels, it is necessary to use a complex measuring (test) composite signal. Requirements for the measuring signal are determined by the features of the discrete-quantized representation of speech signals. It is proposed to use a periodic pulse sequence of a triangular shape as a measuring signal. The triangular measurement signal has an advantage over the harmonic signal in the quantization noise extraction process, since allows you to achieve higher accuracy when processing it. To assess the security of the channel due to pulse-amplitude modulation, a harmonic signal is used, formed from a periodic pulse sequence of a triangular shape by the Fourier transform method. The use of the proposed measuring composite signal makes it possible to establish its numerical dependence with the numerical value of the signal taken as normalized and compare it to make a decision about the security of the speech signal. The materials presented in the article are original and can be used to assess the security of the channels of leakage of speech signals converted into digital form. In addition, the results obtained make it possible to carry out further studies of the security of speech signals during their reverse conversion from digital form to the original signal.

Keywords: information security, speech information leakage channel, discrete-quantized, composite signal.

Conflict of interests. The authors declare no conflict of interests.

For citation. Zheleznjak V.K., Lavrov S.V., Filipovich A.G., Baranouski M.M. Synthesis of a measuring composite signal for assessing the security of speech signals during discrete-quantized transformation. Doklady BGUIR. 2020; 18(6): 81-87.

Введение

Принципы оценки защищенности информационных систем отличаются назначением, видами сигналов, физическими полями рассеивания, каналами утечки информации (КУИ). Информационные системы (ИС) определяются структурами, их составными элементами, параметрами, взаимосвязями между ними, условиями применения, внешними воздействиями. Это позволяет сформировать обобщенную модель защиты информации (ЗИ), которую реализуют схемно-конструктивными решениями.

Защиту ИС синтезируют с помощью обобщенной модели ЗИ [1] на основании анализа оптимизированных, защищенных от утечки системных элементов и внедрением эмерджентных свойств, что позволяет сформулировать методы, принципы, средства защиты информации и их оценки от утечки информации.

Технической защите от утечки аналоговой речевой информации посвящена работа [2].

Передача дискретно-квантованным представлением высокочастотных речевых сигналов по высокоскоростным широкополосным каналам систем связи обусловливает

необходимость обоснования и практической реализации защищенности их от утечки по техническим каналам.

Цель работы – системно проанализировать и обобщить высокоточный измерительный сигнал для оценки защищенности в каналах утечки в шумах высокого уровня дискретно-квантованным представлением речевых сигналов принципами амплитудно-импульсной модуляции (АИМ), реализующим высокочастотную высокоскоростную передачу по широкополосным каналам систем связи.

В работе [1] разработана обобщенная модель защиты информации, в которой анализируются информационные поля рассеивания, формирующие КУИ информационных систем. Нормативный сигнал защищенности канала утечки речевой информации установлен как гармонический измерительный сигнал по СТБ 34.101.29-2011. Для защиты от утечки информации в [1] перечислены новые решения с использованием:

– сигнала линейно-частотной модуляции с преобразованием Вигнера [3];

– сигнала линейно-частотной модуляции с частотно-временным преобразованием [4];

– меандровой последовательности для оценки защищенности от утечки речевых сигналов, преобразованных в битовую последовательность [5];

– частотно-модулированного сигнала без разрыва фазы для оценки речевых сигналов, преобразованных в цифровую форму [5];

– системы измерительной автоматизированной (СИА), которая осуществляет сбор первичной измерительной информации в КУ речевой информации (акустический, виброакустический, электроакустический, магнитный, электрический, электромагнитного поля, наводок полей рассеивания на цепи управления, питания и заземления), оценивает величину разборчивости речи в КУИ по нормативно-методическим требованиям, обеспечивая полноту оценки защищенности объектов информатизации [2].

В работе [6] предложен гармонический измерительный сигнал для оценки защищенности по высокочастотному КУИ при АИМ-сигнале в широкополосных высокочастотных каналах систем связи из сформированной периодической импульсной последовательности треугольной формы. На основании тонкой структуры АИМ-сигнала выделяют исходный речевой сигнал с помощью оценки отношения «сигнал – шум» гармонического измерительного сигнала при максимальной чувствительности при его обработке.

Требования к измерительным сигналам для оценки защищенности речевых сигналов при дискретно-квантованном преобразовании

Дискретно-квантованное представление речевых сигналов осуществляют заменой непрерывной шкалы мгновенных значений непрерывного сигнала дискретной шкалой линейно-ломаной аппроксимации.

Квантующее устройство является основным преобразующим устройством, содержащим линейный и нелинейный элементы [7]. В этой связи квантующее устройство представляет собой совокупность элементов, параметров и связей между ними, исключая избыточные связи, которая обладает эмерджентными свойствами. Идеальным квантирующим устройством является нелинейное устройство с нулевой памятью, передаточная характеристика которой представлена ступенчатой функцией с интервалами квантования входного сигнала Δ, находящимися в однозначных соотношениях с кодирующим входным цифровым сигналом с систематической ошибкой квантования, присущей квантирующему устройству. Она равна $\pm\frac{\Delta}{2}$ при среднем значении, равном нулю. Среднеквадратическое значение $\sigma=\frac{\Delta}{2\sqrt{3}}$, плотность вероятности систематической ошибки квантования равна $\frac{1}{\Delta}$ [8].

Дискретизация сигнала состоит в замене непрерывного сигнала теми или иными дискретными значениями по времени, по уровню либо по времени и уровню.

Дискретизация по времени соответствует выделению значений сигнала в заранее фиксированные моменты времени *T*, где *T* – период периодической последовательности

прямоугольных импульсов [7]. Квантование по уровню соответствует времени сигнала при достижении им заранее достигнутых уровней, отстоящих друг от друга на постоянную величину Δ, где Δ – интервал квантования. Дискретизация сигнала по времени и квантование по уровню соответствуют выделению в заранее фиксированные моменты времени значений непрерывного сигнала, ближайших к фиксированным уровням квантования [7].

Дискретизация по времени заменяет непрерывную функцию решетчатой, которая определяет совокупность выделенных ординат или дискрет [7]. Функция решетчатая – функция, значения которой определены только при дискретных значениях аргумента. Если задана непрерывная функция времени $f(t)$, то ее среднее значение при дискретных значениях аргумента $t = t_n$ преобразуется в решетчатую функцию $f(t_n)$. Разность двух соседних значений аргумента $T_n = t_{n+1} - t_n$ ($t_{n+1} > t_n$) определяет интервал дискретизации (период повторения) по времени, где $n = 1, 2, \ldots m$ [9].

Дискретизация по времени и модуляция осуществляются импульсным модулятором. Входной величиной импульсного модулятора является непрерывная величина входного сигнала, выходной – модулированная последовательность импульсов. При АИМ амплитуды импульсов изменяются по закону модулирующего входного непрерывного сигнала $x(t)$, если на него воздействует периодическая последовательность импульсов [6], на выходе сформирован сигнал решетчатой функции $x(nT)$ при $t = nT$. При подаче на вход гармонического сигнала формируется дискретно-квантованный сигнал [6]. При равномерном квантовании по уровню, из-за нелинейности гармонического сигнала по форме, шум квантования не является равномерным в течение периода гармонического сигнала. Для формирования шума квантования с равномерным периодом повторения линейной амплитудной характеристикой предложено использовать сигнал периодической импульсной последовательности треугольной формы с возможностью оценки мощности сигнала к мощности шума квантования.

Синтез измерительного композитного сигнала

Для формирования измерительного композитного сигнала в качестве исходного сигнала используем периодическую импульсную последовательность прямоугольной формы (рис. 1) с периодом T, равным $1/F_i$, где F_i – средняя частота полосы, равной разборчивости речевого сигнала, $i = \overline{1,n}$ $n = 20$ [10], длительность импульса $\tau = \frac{T}{2}$, F_i = 250; 500; 650; 800; 950; 1125; 1300; 1500; 1700; 1875; 2050; 2250; 2425; 2725; 3100; 3500; 3850; 4550; 6150; 8600 Гц.

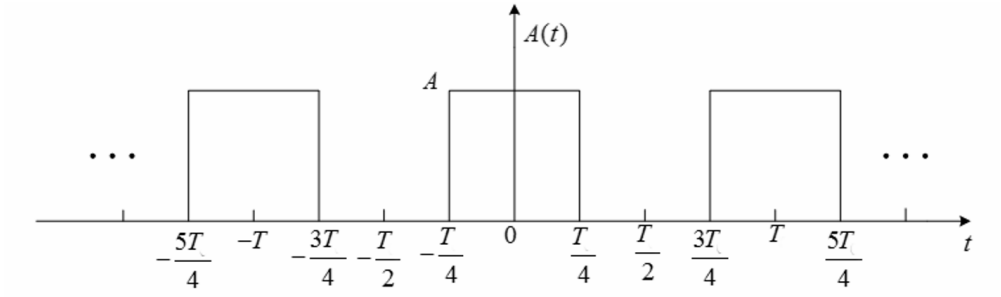

Рис. 1. Последовательность прямоугольных импульсов
Fig. 1. The sequence of rectangular pulses

Разложение периодической последовательности прямоугольных импульсов в ряд Фурье имеет следующий вид [11]:

$$f(t) = \frac{4A}{\pi}\sum_{k=1}^{\infty}\frac{\sin k\omega t}{k}, \qquad (1)$$

где A – амплитуда сигнала; k – номер гармоники (k=1,3,5,…); $\omega = \frac{2\pi}{T_{\text{П}}}$ – угловая частота сигнала; $T_{\text{П}}$ – период сигнала.

Преобразуем автокорреляционной функцией (АКФ) периодическую импульсную последовательность прямоугольной формы в периодическую импульсную последовательность треугольной формы. В результате преобразования получим необходимый измерительный композитный (от английского composite – составной) сигнал, представленный в виде периодической импульсной последовательности треугольной формы с мощностью $A^2\tau$ и длительностью импульса 2τ [12], где A – амплитуда импульса импульсной последовательности прямоугольной формы и τ = 1000; 769; 625; 526; 444; 385; 333; 294; 267; 243; 222; 206; 183; 161; 143; 130; 110; 81; 58 мкс (рис. 2).

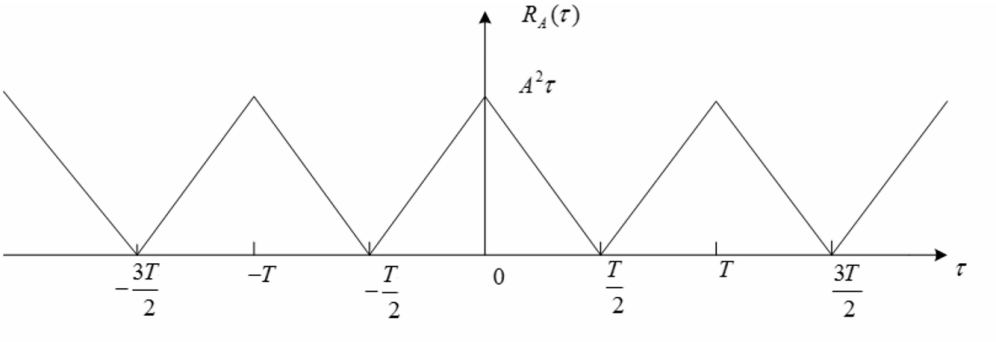

Рис. 2. Автокорреляционная функция
Fig. 2. Autocorrelation function

Разложение периодической импульсной последовательность треугольной формы в ряд Фурье имеет следующий вид [11]:

$$f(t) = \frac{8A}{\pi^2}\sum_{k=1}^{\infty}(-1)^{\frac{k-1}{2}}\frac{\sin k\omega t}{k^2}. \qquad (2)$$

Из формул (1) и (2) видно, что в отличие от периодической последовательности прямоугольных импульсов для периодической импульсной последовательности треугольной формы четные гармоники отсутствуют, а амплитуды нечетных гармоник убывают пропорционально второй степени номеров гармоник, что позволяет производить оценку защищенности по первой (основной) гармонике. Для этого полученный сигнал периодической импульсной последовательности треугольной формы без его искажения вводят в канал передачи речевого сигнала. На выходе канала передачи получают преобразованный сигнал в виде выборки и ошибки квантования, которые обрабатывают в каждой из полос равной разборчивости. Из периодической импульсной последовательности треугольной формы выделяют спектральные составляющие методом преобразования Фурье с получением основной гармоники гармонического сигнала. Оценку защищенности речевого сигнала выполняют сравнением полученного отношения сигнал/шум с нормированным [6].

Заключение

Таким образом, для оценки защищенности канала утечки речевых сигналов при дискретно-квантованном преобразовании предложено использование измерительного композитного сигнала. Предложен способ синтеза измерительного композитного сигнала, представленного в виде периодической импульсной последовательности треугольной формы, формируемой из периодической последовательности прямоугольных импульсов путем последовательного автокорреляционного преобразования. Использование предложенного измерительного композитного сигнала позволяет установить его численную зависимость с численным значением сигнала, принятого в качестве нормированного, и сравнить для принятия решения о защищенности речевого сигнала в КУИ. Полученные результаты позволяют проводить дальнейшие исследования защищенности речевых сигналов при их обратном преобразовании из цифровой формы в исходный сигнал.

Список литературы

1. Железняк В.К., Рябенко Д.С., Лавров С.В. Системный подход: защита информации, помехозащищенность, помехоустойчивость. *Вестник Полоцкого государственного университета.* 2016;4:2-7.
2. Железняк В.К. *Защита информации от утечки по техническим каналам*. Санкт-Петербург: ГУАП; 2006.
3. Железняк В.К., Раханов К.Я. Цифровая обработка сигналов с линейно-частотной модуляцией частотно-временным преобразованием Вигнера для оценки разборчивости речи. *Вестник Полоцкого государственного университета.* 2019;4:16-26.
4. Бураченок И.Б. Железняк В.К. Частотно-временные характеристики широкополосных ЛЧМ-сигналов в полосах равной разборчивости. *Вестник Полоцкого государственного университета.* 2015;12:7-11.
5. Железняк В.К., Рябенко Д.С., Бураченок И.Б. Оценка нормативных показателей защищенности речевого сигнала в аналоговой и цифровой форме. *Современные средства связи: материалы XX международной научно-практической конференции*. 2015;142-144.
6. Железняк В.К., Лавров С.В., Барановский М.М., Филиппович А.Г. Математическая модель каналов утечки речевых сигналов при дискретно-квантованном преобразовании. *Доклады БГУИР*. 2020;18(4):89-95.
7. Цыпкин Я.З. *Основы теории автоматических систем.* Москва: Наука; 1977.
8. Бартон Д.К., Вард Г.Р. *Справочник по радиолокационным измерениям.* Москва: Советское радио; 1976.
9. Колесник В.Д., Полтырев Г.Ш. *Курс теории информации*. Москва: Наука; 1992.
10. Железняк В.К., Бурачёнок И.Б., Рябенко Д.В. Критерии оценки защищенности от утечки речевых сигналов. *Известия Национальной академии наук Беларуси.* 2017;1:122-128.
11. Скляр Б. *Цифровая связь. Теоретические основы и практическое приложение.* Москва: Вильямс; 2007.
12. Стейн С., Джонс. Дж. *Принципы современной теории связи и их применение к передаче дискретных сообщений*. Москва: Связь; 1971.

References

1. Zheleznjak V.K., Ryabenko D.S., Lavrov S.V. [System approach: information protection, noise immunity, noise stability]. *Herald of Polotsk State University*. 2016;4:2-7. (In Russ.)
2. Zheleznjak V.K. [*Information leakage protection through technical channels*]. St. Petersburg: SUAI, 2006. (In Russ.)
3. Zheleznjak V.K., Rahanov K.Ya. [Digital treatment of a signal with linear-frequency modulation of frequency-temporary transformation of wigner to estimate the curability of speech]. *Herald of Polotsk State University.* 2019;4:16-26. (In Russ.)
4. Zheleznjak V.K., Burachonak I.B. [Time-frequency features of broadband chirp signals in the bands of equal intelligibility]. *Herald of Polotsk State University*. 2015;12:7-11. (In Russ.)
5. Ryabenko D.S., Zheleznjak V.K., Burachonak I.B. [Assessment of standard indicators of the security of a speech signal in analog and digital form]. *Modern means of communication: materials of the XX international scientific and practical conference.* 2015;142-144. (In Russ.)
6. Zheleznjak V.K., Lavrov S.V., Baranouski M.M., Filipovich A.G. [Mathematical model of speech signal leakage channels during discrete-quantified conversion]. *Doklady BGUIR = Doklady BGUIR*. 2020;18(4):89-95. (In Russ.)
7. Tsypkin Ya.Z. [*Foundations of the theory of automatic systems*]. Moscow: Science; 1977. (In Russ.)
8. Barton D.C., Ward G.R. [*Handbook of radar measurements*]. Moscow: Soviet radio; 1976. (In Russ.)
9. Kolesnik V.D., Poltyrev G.Sh. [*Information theory course*]. Moscow: Science; 1992. (In Russ.)
10. Zheleznjak V.K., Burachonak I.B., Ryabenko D.S. [Assessment criteria of voice signal leakage protection]. *Proceedings of the National Academy of Sciences of Belarus*. 2017;1:122-128. (In Russ.)
11. Sklyar B. [*Digital communication. Theoretical foundations and practical application*]. Moscow: Williams; 2007. (In Russ.)
12. Stein S., Jones. J. [*Principles of modern communication theory and their application to the transmission of discrete messages*]. Moscow: Communication; 1971. (In Russ.)

Вклад авторов

Железняк В.К. определил замысел исследования, осуществил окончательное утверждение рукописи для публикации, ее критический пересмотр в части значимого интеллектуального содержания.

Лавров С.В. принимал участие в разработке способа синтеза композитного сигнала и интерпретации полученных результатов.

Филиппович А.Г. осуществил критический пересмотр статьи в части значимого интеллектуального содержания, вносил правки в текст статьи.

Барановский М.М. принимал участие в разработке способа синтеза композитного сигнала и интерпретации полученных результатов, осуществил редактирование и оформление статьи для публикации.

Authors' contribution

Zheleznjak V.K. defined the concept of research, delivered the final approval of the manuscript for publication, including its critical review in part of significant intellectual content.

Lavrov S.V. participated in the development of a method of synthesis of the composite signal and interpret the results.

Filipovich A.G. included its critical review in part of significant intellectual content, edited the text of the article.

Baranouski M.M. participated in the development of a method for the synthesis of a composite signal and participated in the interpretation of the results, prepared the article for publication.

Сведения об авторах

Железняк В.К., д.т.н., профессор, заведующий опытно-экспериментальной лабораторией технической защиты информации Полоцкого государственного университета.

Лавров С.В., аспирант Полоцкого государственного университета.

Филиппович А.Г., к.т.н., главный специалист Оперативно-аналитического центра при Президенте Республики Беларусь.

Барановский М.М., главный специалист Оперативно-аналитического центра при Президенте Республики Беларусь.

Information about the authors

Zheleznjak V.K., D.Sci., Professor, Head of the Research Experimental Laboratory of Technical Information Protection of Polotsk State University.

Lavrov S.V., PG Student of Polotsk State University.

Filipovich A.G., PhD, Chief Specialist of the Operational and Analytical Center under the Aegis of the President of the Republic of Belarus.

Baranouski M.M., Chief Specialist of the Operational and Analytical Center under the Aegis of the President of the Republic of Belarus.

Адрес для корреспонденции

211440, Республика Беларусь,
Витебская обл., г. Новополоцк, ул. Блохина, 29,
Полоцкий государственный университет
тел. +375-29-212-74-47;
e-mail: v.zheleznjak@psu.by
Железняк Владимир Кириллович

Address for correspondence

211440, Republic of Belarus,
Vitebsk region, Novopolotsk, Blokhina str., 29,
Polotsk State University
tel. +375-29-212-74-47;
e-mail: v.zheleznjak@psu.by
Zheleznjak Vladimir Kirilovich